

Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name: FPO > VHA > EES > LAN (Salt Lake City)

OMB Unique System / Application / Program

Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Each VA facility uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including supply management, decision support, and education.

Description of System / Application / Program:

Facility Name: Employee Education System

Title:	Name:	Phone:	Email:
Privacy Officer:	Norman Sealy	202-380-3597	norman.sealy@va.gov
Information Security Officer:	Janet Garleb	314-894-6468	janet.garleb@va.gov
Chief Information Officer:	Joseph Schaefer	440-526-3030 x	joseph.schaefer@va.gov
Person Completing Document:	Janet Garleb	314-894-6468	janet.garleb@va.gov
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) 08/2009

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Statutory provisions, Executive Order 12191 (45 FR 7997 (Feb. 6, 1980)) and other Executive Orders of the President, and rules and regulations of certain Federal regulatory departments and agencies.

What is the expected number of individuals that will have their PII stored in this system:

250,000

Identify what stage the System / Application / Program is at:

Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

01/1998

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Has a PIA been completed within the last three years?

Yes

Date of Report (MM/YYYY): 01/2010

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☐ Have any changes been made to the system since the last PIA?
- ☒ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☐ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

☒ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

27VA047

2. Name of the System of Records:

Personnel and Accounting Pay System - VA

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

[Dept of VA Privacy Act System of Records,
http://www.rms.oit.va.gov/sor_records.asp](http://www.rms.oit.va.gov/sor_records.asp)

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

No

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	Maintaining training record	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information				
Guardian Information	N/A			
Education Information	Paper & Electronic	Maintaining training record	Written	Written
Benefit Information	N/A			
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Other (Explain)	Voluntary	On the form - veteran or patient data is not collected
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	Yes	Other (Explain)	Voluntary	On the form - veteran or patient data is not collected

Benefit Information	No
Other (Explain)	
Other (Explain)	
Other (Explain)	

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Security	No	VA Form 711 for PIV	PII	PIV
Other Veteran Organization	N/A				
Other Federal Government Agency	N/A				
State Government Agency	N/A				
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system:

Per responses in Tab 4, does the system gather information from an individual? Yes

If information is gathered from an individual, is the information provided:

- ☒ Through a Written Request
- ☒ Submitted in Person
- ☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down? Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? No

if yes, please check all that apply:

- ☐ Drug/Alcohol Counseling
- ☐ Mental Health
- ☐ HIV
- ☐ Research
- ☐ Sickle Cell
- ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

All forms, both paper and online, specifically ask for only the data needed from the individuals to be entered by them in order to provide that individual with appropriate credit for the course.

Answer:

How is data checked for completeness?

Answer:

Project team reviews the data for accuracy.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

As part of the registration process the information is validated and for existing records updated as appropriated by project team.

How is new data verified for relevance, authenticity and accuracy?

Answer:

Project team reviews the data for accuracy.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer:

Data records are maintained for 7 years

Explain why the information is needed for the indicated retention period?

Answer:

To meet clinical accreditation requirements

What are the procedures for eliminating data at the end of the retention period?

Answer:

Paper records are shredded,
electronic records are
deleted, and media records
are destroyed or shredded.

Where are these procedures documented?

Answer:

Procedures for maintenance
of the records are contained
in EES policy #777-EDU018-
06. EES has and will
continue to follow
government regulations
regarding destruction of
records containing PII. A
policy regarding records
management is being
drafted and will include
guidance for destruction of
the records.

How are data retention procedures enforced?

Answer:

Annual review

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

No

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

Answer:

Information and Technology (OI&T) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that LAN is and has been subject to. In addition, OI&T administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the LAN project level -The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53)), as well as identified security weaknesses that must be corrected. Minimum security controls for a moderate system are operational in

Explain how the project meets IT security requirements and procedures required by federal law.

Answer:

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- | | |
|--------------------------------------------------------------------------|----------------------------------------------------------------|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Computer Misuse |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Substance Abuse |
| <input type="checkbox"/> Data Destruction | <input type="checkbox"/> Theft of Assets |
| <input type="checkbox"/> Data Disclosure | <input type="checkbox"/> Theft of Data |
| <input type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Vandalism/Rioting |
| <input type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Errors (Configuration and Data Entry) |
| <input checked="" type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Burglary/Break In/Robbery |
| <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement |
| <input checked="" type="checkbox"/> Flooding/Water Damage | |

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- | | |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Risk Management | <input checked="" type="checkbox"/> Audit and Accountability |
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Configuration Management |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Incident Response |
| <input checked="" type="checkbox"/> Physical and Environmental Protection | <input checked="" type="checkbox"/> Media Protection |
| <input checked="" type="checkbox"/> Personnel Security | |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: Continuous review of data collection processes are needed

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?

(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☒ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?

(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☒ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?

(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☒ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments? Yes

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Yes

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System Veterans Assistance Discharge System (VADS)	Education Training Website	Appraisal System Web Electronic Lender Identification
LGY Processing	VR&E Training Website VA Reserve Educational Assistance Program	CONDO PUD Builder Centralized Property Tracking System
Loan Service and Claims LGY Home Loans	Web Automated Verification of Enrollment Right Now Web VA Online Certification of Enrollment (VA-ONCE)	Electronic Appraisal System
Search Participant Profile (SPP)	Automated Folder Processing System (AFPS)	Web LGY
Control of Veterans Records (COVERS)	Personal Computer Generated Letters (PCGL)	Access Manager
SHARE Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	SAHSHA
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	VBA Data Warehouse Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry) VBA Enterprise Messaging System
Awards	State Benefits Reference System Training and Performance Support System (TPSS)	LGY Centralized Fax System
Financial and Accounting System (FAS)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ) Automated Sales Reporting (ASR)
Eligibility Verification Report (EVR) Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM) Web Service Medical Records (WebSMR)	Compensation and Pension (C&P) Record Interchange (CAPRI) Control of Veterans Records (COVERS)	Purchase Order Management System (POMS)
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Veterans Canteen Web
Fiduciary STAR Case Review Veterans Exam Request Info System (VERIS)	Fiduciary Beneficiary System (FBS)	Inventory Management System (IMS)
Web Automated Folder Processing System (WAFPS)	Hearing Officer Letters and Reports System (HOLAR)	Synquest
	Inforce	RAI/MDS
		ASSISTS
Courseware Delivery System (CDS) Electronic Performance Support System (EPSS)	Awards	MUSE
Veterans Service Representative (VSR) Advisor	Actuarial	Bbraun (CP Hemo)
	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	<table><tr><td>Name</td><td></td><td>Description</td><td></td><td>Comments</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Name		Description		Comments					<table><tr><td><input type="checkbox"/></td><td>Is PII collected by this min or application?</td></tr><tr><td><input type="checkbox"/></td><td>Does this minor application store PII?</td></tr><tr><td></td><td>If yes, where?</td></tr><tr><td></td><td>Who has access to this data?</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>	<input type="checkbox"/>	Is PII collected by this min or application?	<input type="checkbox"/>	Does this minor application store PII?		If yes, where?		Who has access to this data?				
	Name		Description		Comments																		
	<input type="checkbox"/>	Is PII collected by this min or application?																					
	<input type="checkbox"/>	Does this minor application store PII?																					
		If yes, where?																					
	Who has access to this data?																						

Minor app #2	<table><tr><td>Name</td><td></td><td>Description</td><td></td><td>Comments</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Name		Description		Comments					<table><tr><td><input type="checkbox"/></td><td>Is PII collected by this min or application?</td></tr><tr><td><input type="checkbox"/></td><td>Does this minor application store PII?</td></tr><tr><td></td><td>If yes, where?</td></tr><tr><td></td><td>Who has access to this data?</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>	<input type="checkbox"/>	Is PII collected by this min or application?	<input type="checkbox"/>	Does this minor application store PII?		If yes, where?		Who has access to this data?				
	Name		Description		Comments																		
	<input type="checkbox"/>	Is PII collected by this min or application?																					
	<input type="checkbox"/>	Does this minor application store PII?																					
		If yes, where?																					
	Who has access to this data?																						

Minor app #3	<table><tr><td>Name</td><td></td><td>Description</td><td></td><td>Comments</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Name		Description		Comments					<table><tr><td><input type="checkbox"/></td><td>Is PII collected by this min or application?</td></tr><tr><td><input type="checkbox"/></td><td>Does this minor application store PII?</td></tr><tr><td></td><td>If yes, where?</td></tr><tr><td></td><td>Who has access to this data?</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>	<input type="checkbox"/>	Is PII collected by this min or application?	<input type="checkbox"/>	Does this minor application store PII?		If yes, where?		Who has access to this data?				
	Name		Description		Comments																		
	<input type="checkbox"/>	Is PII collected by this min or application?																					
	<input type="checkbox"/>	Does this minor application store PII?																					
		If yes, where?																					
	Who has access to this data?																						

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus	BIRLS
Mental Health Asisstant	Centralized Accounts Receivable System (CARS)
Telecare Record Manager	
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitelment Program for Survivors (REAPS) Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	SUPPORT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION	KIDS
AUTOMATED LAB INSTRUMENTS	SYSTEM	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EQUIPMENT/TURN-IN	LETTERMAN
BAR CODE MED ADMIN	REQUEST	LEXICON UTILITY
BED CONTROL	EVENT CAPTURE	LIBRARY
BENEFICIARY TRAVEL	EVENT DRIVEN REPORTING	LIST MANAGER
CAPACITY MANAGEMENT - RUM	EXTENSIBLE EDITOR	MAILMAN
CAPRI	EXTERNAL PEER REVIEW	MASTER PATIENT INDEX
CAPACITY MANAGEMENT TOOLS	FEE BASIS	VISTA
CARE MANAGEMENT	FUNCTIONAL	MCCR NATIONAL
CLINICAL CASE REGISTRIES	INDEPENDENCE	DATABASE
CLINICAL INFO RESOURCE NETWORK	GEN. MED. REC. - GENERATOR	MEDICINE
CLINICAL MONITORING SYSTEM	GEN. MED. REC. - I/O	MENTAL HEALTH
CLINICAL PROCEDURES	GEN. MED. REC. - VITALS	
CLINICAL REMINDERS	GENERIC CODE SHEET	MICOM
CMOP	GRECC	MINIMAL PATIENT
CONSULT/REQUEST TRACKING	HEALTH DATA &	DATASET
CONTROLLED SUBSTANCES	INFORMATICS	MYHEALTHVET
CPT/HCPCS CODES	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)
CREDENTIALS TRACKING	HEALTH SUMMARY	A4EL
DENTAL	HINQ	NATIONAL DRUG FILE
DIETETICS	HOSPITAL BASED HOME	NATIONAL LABORATORY
DISCHARGE SUMMARY	CARE	TEST
DRG GROUPER	ICR - IMMUNOLOGY CASE	NDBI
	REGISTRY	NETWORK HEALTH
	IFCAP	EXCHANGE
	IMAGING	NOIS
	INCIDENT REPORTING	NURSING SERVICE
	INCOME VERIFICATION	OCCURRENCE SCREEN
	MATCH	ONCOLOGY
	INCOMPLETE RECORDS	ORDER ENTRY/RESULTS
	TRACKING	REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #2	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #3	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECS
PRACTICE	
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING
MEDICINE	
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name		Description		Comments	
	Tracking Continuing Education (TRACE)		Workflow management and training tracking tool		Archived data only - no longer ask for SSN (full or partial) or DOB.	
		YES	Is PII collected by this min or application?			
		YES	Does this minor application store PII?			
			If yes, where? VA Intranet based database			
			Who has access to this data? VA Learning University and Employee Education System staff. Level of access is restricted based on duty requirements.			

Minor app #2	Name		Description		Comments	
	VA Conference Registration (VACR)		Registration and support tool for large conference		In the process of removing last four of SSN from registration process.	
		YES	Is PII collected by this min or application?			
		YES	Does this minor application store PII?			
			If yes, where? VA Intranet based database			
			Who has access to this data? VA Learning University and Employee Education System staff. Level of access is restricted based on duty requirements.			

Minor app #3	Name		Description		Comments	
	Scanning Exam and Evaluation System (SEES)		Survey, examinations and evaluations to support VALU		PII is not collected on the majority of the evaluation	
		YES	Is PII collected by this min or application?			
		YES	Does this minor application store PII?			
			If yes, where? VA Intranet based database			
			Who has access to this data? VA Learning University and Employee Education System staff. Level of access is restricted based on duty requirements.			

(FY 2010) PIA: Final Signatures

Facility Name: Employee Education System

Title:	Name:	Phone:	Email:
Privacy Officer:	Norman Sealy	202-380-3597	norman.sealy@va.gov
Digital Signature Block			
Information Security Officer:	Janet Garleb	314-894-6468	janet.garleb@va.gov
Digital Signature Block			
Chief Information Officer:	Joseph Schaefer	440-526-3030 x6647	joseph.schaefer@va.gov
Digital Signature Block			
Person Completing Document:	Janet Garleb	314-894-6468	janet.garleb@va.gov
Digital Signature Block			
System / Application / Program Manager:	0	0	0
Digital Signature Block			

Date of Report: 1/20/2010

OMB Unique Project Identifier 029-00-02-00-01-1120-00

Project Name FPO > VHA > EES > LAN (Salt Lake City)